1 SYSTEM ENABLING THE ESTABLISHMENT OF A TELNET CONNECTION TO

2 A REMOTE DEVICE NOT PROVIDED WITH A MODEM

3

4

5 Technical Field

6

7 The present invention relates generally to data transmission systems wherein a

8 help desk workstation can establish a Telnet connection through a data

9 transmission network enabling it to use a telephone line to gain access to an IP

10 device and relates in particular to a system enabling the establishment of a

11 Telnet connection with a remote device not provided with a modem.

12

13 Background

14

15 In managed network services, a service provider manages the customer

16 equipment such as access routers. It generally can gain access to this equipment

17 via one of the network links or through a dial connection via PSTN or ISDN if

18 such a connection is available on the equipment. The main protocol used to

19 control, configure and manage for this equipment is called Telnet which is pre-

20 installed on several platforms such as windows 95/98/NT/2000/XP and UNIX

21 operating systems. Telnet is a standard protocol that is a kind of remote login

22 function.

23

24 For a user, to Telnet to a host or device means to establish a connection through

25 a network to this host or device. This connection is feasible through an IP

26 network directly using the IP address or name of the Host or using the dial

27 number of the IP device. Telnet allows a user to use his telephone line to gain

28 access to and control of a remote PC/Server or any IP device having a dial

29 connection.

30

1   Telneting to a computer allows the user to control it directly. When the user

2   telnets into a remote device it is as if he was sitting at a terminal and keyboard

3   directly connected to the system. To do this, the user must have access to an

4   account that he is allowed to use. Usually, an account on the remote host is

5   required to be able to login to it once a connection is established.

6

7   Several Telnet programs can be used and some are included in Operating

8   systems such as "Hyperterminal" for Windows platforms. When the program is

9   started, it asks the user for a host. Then the host asks for a login name and

10   password. If the user is registered, and has an account, he will be able to log in.

11

12   This explains that the Telnet access to customer located devices is a must for

13   service providers in order to manage these devices. In Broadband Internet, only

14   one connection from the router to the network is provided on low cost routers. It

15   can be for example a native DSL / Cable connection or Ethernet router device.

16   No dial backup or dial port for configuration and maintenance is provided and the

17   only serial port is generally the console port. The console port is an

18   asynchronous serial port that can be used for Telnet but is not well protected by

19   passwords. Adding one modem connection to the router on this console port is

20   expensive insofar as a secure external modem with built-in authentication is

21   required since the port is the console port allowing access without authentication.

22

23   When the router is not a managed router but under the user responsibility, there

24   is no problem since the user can manage it either from the LAN side Ethernet

25   port or the console port. But, when a service provider manages the router, it

26   becomes more complex and expensive to use a low cost router due to the

27   additional expensive modem.

28

29   Today, an external modem is required on such low cost routers and since the

30   console port is the only port, there is a security issue, which requires using a very

31   secure modem with integrated authentication. An existing alternate solution is to

1   use PCs to access locally attached routers but this remote control can only be

2   done by tools that get full control of the PC such as "Carbon Copy" or "Desktop

3   on-call". There is a user security issue since, if it is normal for the user to get full

4   PC control, it is not conceivable that a customer allows a provider to do it. Today,

5   there are only tools that give a full control of the operating system of the PC.

6   These tools are very efficient but have several drawbacks, which prevent from

7   using them in this environment. The main drawback is the security since the

8   service provider help desk will have access to the full system of the customer.

9   Generally, a customer does not like to allow access to a PC on which confidential

10   information may be stored. In addition, it is not possible to ensure that no injury

11   will be done by mistake or by people that will gain access to system using the

12   dial port. Another drawback is the overhead and performance impact on the

13   system since the system is no longer under control of the customer.

14

15   Summary of the Invention

16

17   Accordingly, the main object of the invention is to achieve a method and to

18   provide a system wherein a user workstation includes a Telnet proxy function

19   enabling a Telnet connection between a Telnet client and a remote device not

20   provided with a modem.

21

22   The invention relates therefore to a data transmission system comprising a help

23   desk workstation provided with the Telnet client function and connected to a

24   Wide Area Network WAN and to the Public Switched Telephone Network PSTN,

25   and a Telnet manageable device not provided with a modem and to which the

26   help desk workstation may gain access by using the Telnet protocol. The system

27   comprises a data processing device provided with the proxy function and being

28   connected to the PSTN and to the Telnet manageable device by the intermediary

29   of a Local Area Network LAN, the data processing device including proxy means

30   for completing a first Telnet connection with the help desk workstation through

31   the PSTN and for establishing a second Telnet connection with the Telnet

1   manageable device upon receiving a request from the help desk workstation to

2   gain the Telnet access to the Telnet manageable device.

3

4   Brief Description of the Drawings

5

6   The above and other objects, features and advantages of the invention will be

7   better understood by reading the following more particular description of the

8   invention in conjunction with the accompanying drawings wherein:

9   Fig. 1 is a schematic block-diagram representing a system involved in a Telnet

10 environment including the proxy function device according to an embodiment of

11 the invention.

12   Fig. 2 is a schematic representation of the basic communication flows between

13 the components involved in the system illustrated in Fig. 1.

14   Fig. 3 is a flow chart representing the steps of the method used to establish the

15 connection with a remote device in the system illustrated in Fig. 1.

16   Fig. 4 is a flow chart representing the steps of the method used by the remote

17 device in response to the establishment of the connection.

18   Fig. 5A and 5B represent respectively the flow charts of the Telnet command

19 process at the Telnet client and at the remote device.

20   Fig. 6 is a diagram representing the Telnet proxy function flows according to

21 another embodiment of the invention.

22

23 Detailed Description of the Invention

24

25 The main idea of the invention is to use a user workstation which is a data

26 processing device as a modem to solve the security issue raised by the access

27 of a help desk workstation to the system of the customer as already mentioned.

28 With an additional Telnet proxy function in the PC of the user workstation, this

29 PC will be equivalent to an isolated modem having no access to the user

30 resources. This will allow the connection via a local LAN or via the COM port to

31 the router or, in a general way, to any kind of Telnet manageable device.

1

2   It is recalled that an application proxy is an application program that runs on a

3   system between two networks. The PC on which the proxy runs does not need

4   to be acting as a router. When a client program establishes a connection

5   "through" a proxy to a destination device, it first establishes a connection directly

6   to the proxy server program. The client then negotiates with the proxy server to

7   make the proxy establish a connection on behalf of the client between the proxy

8   and the destination device. If successful, there are then two connections in

9   place: one between client and the proxy server and another between the proxy

10 server and the destination device. Once established, the proxy then receives

11 and forwards traffic bi-directionally between the Telnet client and the remote

12 device. The proxy makes all connection-establishment and packet-forwarding

13 decisions. Any routing functions that are active on the PC are generally irrelevant

14 to the proxy. In the present invention, the Telnet proxy function is configured for

15 only managing a device such as a router when no direct access is feasible via

16 the Digital Subscriber line (DSL).

17

18 In reference to Fig. 1, a help desk workstation 100, which includes the Telnet

19 client function, is connected to the Public Switched Telephone Network (PSTN)

20 130 and to a WAN 115. Help desk workstation 100 can gain access to a Telnet

21 manageable device 120 through the WAN 115. When this connection fails, an

22 alternate path is required. If no modem is available on device 120, the access to

23 it is then achieved through a data processing device 110 such as an intermediate

24 host or PC on which a Telnet proxy software is implemented. This proxy function

25 is interfaced on the one hand to the modem port 105 connected to PSTN 130

26 and on the other hand to the port linked to LAN 125 itself connected to the device

27 120 in the preferred embodiment. It can be also connected to the COM port of

28 the host for rerouting the Telnet commands as explained below. The Telnet proxy

29 function is therefore implemented on top of the IP stack of the host 110 in order

30 to intercept the IP Telnet packets that use IP port 23 which is associated with the

31 Telnet protocol. Therefore, a user on the help desk workstation 100 can reach

1   the PC 110 via the PSTN 130, and then the proxy function in host 110 allows to

2   telnet the remote device 120 to solve problems when the device 120 cannot be

3   reached from the WAN Network side.

4

5   Note that two cases are possible. In a first embodiment, the Telnet client 100 is a

6   legacy Telnet client, which conforms to the RFC 854. In that case, the proxy is

7   not configured through the help desk workstation and is preconfigured to access

8   its IP default gateway configured in the host IP stack through the LAN interface

9   or through the serial COM port if it is not reachable via the LAN side.

10

11   In a second embodiment, the Telnet client is still a legacy Telnet client. But the

12   proxy is a piece of software that can be user (Host owner) configured to access a

13   defined IP address or list of addresses through the LAN interface or through the

14   serial COM port if it is not reachable via the LAN side.

15

16   The main difference between the first and second embodiment is the way the IP

17   address of the device on which the Telnet will be done is preset. The first

18   embodiment uses the default gateway IP address of the Host on which runs the

19   proxy. This default gateway address corresponds to the router to which each IP

20   packet is sent. It can be preconfigured in the host IP configuration or discovered

21   automatically thanks to DHCP (Dynamic Host Configuration Protocol). In SOHO

22   (Small Office Home Office) environment there is generally only one router or

23   possible gateway so that there is no need to define it manually. The second

24   embodiment does not use this default gateway as preferred IP address for

25   Telnet. A file is built in which the IP address is written by the user. The Telnet will

26   be done using this address which may be different from the default gateway

27   defined and used in the Host IP stack. This may be useful in more complex LAN

28   environment where multiple routers are implemented. It is also possible to define

29   more that one IP address in the list, either to access the same device on another

30   port if such interface exists or to gain access to another device when the first

31   fails.

1

2   The basic flows used to establish a connection are illustrated in Fig. 2. First, the

3   client program in help desk workstation 100 establishes a legacy telnet

4   connection directly to the proxy server program using messages such as

5   MessAtoB Request 200 and Acknowledgment MessBtoA 230 packets. In

6   parallel, for each packet, the proxy function in host 110 establishes a connection

7   using a set of messages MessBtoC 210 and MessCtoB 220 as answers on

8   behalf of the client between the proxy and the destination device 120 using the

9   same packet type with a different IP header. If successful, there are then two

10   connections in place: one between the client and the proxy function and another

11   between the proxy server and the destination device.

12

13   Practically, help desk workstation 100 sends a Telnet "request" message 200 to

14   the Telnet Proxy 110. Then, the Telnet Proxy process stores this message 200

15   and modifies its IP header in "request" message 210 to forward it to device 120.

16   The device 120 sends a "reply message" 220 to Telnet Proxy 110 which checks,

17   processes and translates back this message in a "reply" message 230 before to

18   send it to the Standard Telnet client 100.

19

20   The Telnet proxy method for incoming messages from the Telnet client is now

21   described in reference to Fig. 3. First, the system waits for a telnet message from

22   the help desk workstation (step 300) by scanning the incoming TCP/IP packets

23   on the dial access. When a message arrives, it is checked whether it is received

24   on port 23 associated with the Telnet protocol (step 302). If not, this means that

25   the packet is for another task than the Telnet proxy and the packet is forwarded

26   to the host of the data processing device according a transparent mode (step

27   306). Note that another Telnet application cannot be used in parallel with the

28   proxy function on the same interface.

29

30   If the message is received on port 23, it is checked whether it is a Telnet

31   command (step 308). If not, it is checked whether it corresponds to the phase of

1   initialization for requesting a connection (step 310). If it is not the case, this

2   corresponds to an error and the message is rejected (step 315). If the received

3   message corresponds to the phase of initialization, a connection request is sent

4   to the remote destination device (step 312).

5

6   In case of a message complying with the Telnet protocol, it is checked whether it

7   is really a Telnet command (step 320). If not, the message is rejected (step 315).

8   If so, the command is processed (step 325) as described hereafter and a new

9   Telnet message is forwarded to the Telnet manageable device 120 (step 330).

10   Note that, when the message is rejected, a feedback message is sent to the help

11   desk workstation.

12

13   In the two first embodiments wherein the Telnet client is a legacy Telnet client,

14   the connection request (step 312) is responsible to

15   Get the IP address of the device 120,

16   Get automatically the IP address of LAN interface of device 110, and

17   Create the Telnet connection between the workstation 100 and the device 110,

18   and between the devices 110 and 120.

19

20   But, whereas the IP address of the device 120 corresponds to the default

21   gateway of device 110 in the first embodiment, this IP address has been

22   configured previously in the Telnet proxy program (during the installation for

23   example), in the second embodiment. Note that a rejection message is sent if

24   one of the above steps fails.

25

26   Fig. 4 describes the Telnet proxy process for an incoming message from the

27   device 120 to the proxy function in device 110. First, the system waits for a

28   Telnet message from device 120 (step 400). When a message is received, it is

29   checked whether it is a Telnet command on port 23 as previously (step 420), If

30   not, the message is rejected (step 415) and a feedback message is sent to the

31   source. If it is a Telnet command, the command is processed (step 425) as

1   described hereafter, and a new Telnet message is sent to help desk workstation

2   100 (step 430).

3

4   In reference to Fig. 5A, the processing of a command received from help desk

5   workstation 100 starts from step 500 where the Telnet Command process

6   receives a message from workstation 100. This message goes to the SWAP

7   routine 510 which performs the following modifications in the IP Datagram

8   Header:

9   Change the Source IP address by IP address of host 110,

10   Change the Destination IP address by IP address of device 120.

11   Then, the modified Telnet message 520 is sent to device 120.

12

13   The processing of a message received from the Telnet manageable device 120

14   starts in step 530 where the Telnet Command process receives a message from

15   device 120. This message goes to the SWAP BACK routine 540 which performs

16   the following modifications in the IP Datagram Header:

17   Change the Source IP address by IP address of host 110,

18   Change the Destination IP address by IP address of workstation 100.

19   Then, the modified Telnet message 550 is sent to 100.

20

21   The need to change the Source and destination IP addresses is because a

22   legacy Telnet client needs to know to which device it connects and be configured

23   for that. As the legacy IP stack of the Host is used, the destination IP address

24   used by the Telnet client is the proxy address. The true destination is in fact the

25   destination device and not the device 110, which acts as a proxy. The proxy,

26   therefore, changes on the fly the destination address with the final device

27   address the proxy knows because it is either the default gateway address or the

28   IP address defined in the proxy configuration. Similarly, the proxy has to change

29   the source address of the packet because the incoming source address is the

30   Telnet client address. To get back an answer from the destination device, the

1   source address has to be the proxy, otherwise the destination address will see

2   an unreachable address.

3

4   Fig. 6 shows the flows between involved devices for the more complex solution

5   based on a new Telnet Client that interfaces in a proprietary manner the Telnet

6   proxy function as being referred to a third embodiment of the invention. The

7   advantage of such implementation is to offer better performance and more

8   functionality. The performance increase is due to the aggregation of basic telnet

9   input commands, which is character based into full command messages between

10   the Telnet client 100 and the proxy 110. Then, between host 110 and device

11   120, the commands are converted back to a character transmission mode.

12

13   In addition there is no need to use for telnet between the client and the proxy the

14   IP address of workstation 100 and the IP address of device 110 since a

15   proprietary protocol such as the one detailed hereunder is used. Only the devices

16   110 and 120 will really exchange telnet messages conforming to the IETF RFC

17   854 and will use their own IP addresses as source and destination addresses.

18   The proxy in this embodiment does not have to swap the IP addresses for

19   packets transmitted between the workstation and the proxy function because the

20   telnet commands are encapsulated in the proprietary protocol.

21

22   The proprietary protocol starts with an InitSession message 601 acknowledged

23   by ACK message 621. Then the settings are exchanged to configure properly the

24   telnet session. This starts by a getLocalInfo message 602 and the answer

25   sendLocalInfo622, from host 110, which provides the workstation with the

26   environment from the proxy function. Information transmitted may include

27   Interfaces available, IP stack configuration (WinIPcfg or IPconfig in windows),

28   previous Profile used, results of basic host station IP tests such as ping,

29   traceroute, routing information (ROUTE PRINT in windows 2000 for example).

30   Based on this information, the user using the Telnet client will define to which

31   device and through which interface he will issue the Telnet command and

1   therefore configure device 110 thanks to a sendInitProfile message 603 which

2   allows the telnet proxy function to start a real Telnet session with the destination

3   device by initTelnet 623. Upon reception of the acknowledge from device 120,

4   the proxy function will forward the ACK answer 624 to the workstation 100 which

5   means that Telnet commands can be transmitted.

6

7   Full lines of commands are sent by the workstation using sendCommand

8   messages 605 that are converted by the proxy into a set of character commands

9   messages 625. A similar process is used for device 120 to transmit commands to

10   the workstation 100 but using the reverse method. Device 120 sends character

11   commands using sendCharacter messages 626 aggregated by the proxy

12   function in order to rebuild full commands forwarded to the workstation 100 as

13   sendResult 627 messages. The proxy function uses a timer for character

14   aggregation, which means that sometimes sendResult contains a partial line

15   command with the remaining part on next messages but it has no impact in the

16   functionality of the system.

17

18   Similarly to the Init process, the workstation 100 can initiate a Close session

19   process by sendClosedSession message 608 forwarded to device 120 by the

20   proxy function as ClosedSession 628. The acknowledge message from device

21   120 allows to release the session by releaseSession message 629 from proxy

22   110 to workstation 100.

23

24   It must be noted that, when the connection through the LAN port has failed, it is

25   possible to use the link from serial asynchronous COM port of host 110 (see Fig.

26   1) to the console port on device 120. Upon detection of the failure, a retry Telnet

27   connection may be issued by the help desk administration on workstation 100

28   that will be directed to the COM port of host 110 by the proxy function. An

29   automatic Telnet access attempt through connected COM ports may also be

30   performed after several connection failures via the LAN port if defined within the

31   proxy function. When this is available, the authentication of the user has to be

2002-0149

1   performed within the proxy function of host 110. These options are set during the

2   configuration of the Telnet proxy function.

3